

ERIE 1 BOCES POLICY SERVICES

SPECIAL ALERT - June 2014

Data Privacy and Security

As you may know, on March 31st of this year the state legislature passed the Common Core Implementation Reform Act as part of its annual budget. The Act includes a series of revisions to Education Law impacting student assessments, student promotion and retention, APPR, instruction, professional development, and data privacy and security. A number of districts have expressed particular interest in provisions of a newly adopted Education Law Section 2-d affecting student and educator data privacy and security. This Alert discusses relevant pieces of the legislation and informs subscribing districts of Policy Services' plans moving forward.

Introduction

Education Law Section 2-d governs the release of student and educator personally identifiable information. In so doing, it strengthens the protection of such data through six related measures: (1) creating the position of Chief Privacy Officer within the State Education Department (SED); (2) requiring that each educational agency adopt a parents bill of rights for data privacy and security; (3) promoting the least intrusive data collection policies practicable; (4) requiring that educational agencies adopt data security and privacy policies consistent with state and federal law; (5) regulating disclosure of personally identifiable information to third party contractors; and (6) providing mechanisms for addressing unauthorized disclosure of personally identifiable information by third party contractors. These provisions will be addressed in turn, with particular emphasis on the parents bill of rights and data security and privacy policies.

Chief Privacy Officer

Pursuant to Section 2-d(2), the Commissioner of Education is required to appoint a "Chief Privacy Officer" to serve within the SED for a period of three (3) years. The Chief Privacy Officer's duties include, but are not limited to: promoting the implementation of sound data privacy and security practices; providing assistance to educational agencies regarding minimum standards and best practices for ensuring data privacy and security; and assisting the Commissioner in establishing a protocol for the submission of complaints related to data security breaches. See Education Law § 2-d(2)(b). Importantly, the Chief Privacy Officer will also be involved in developing elements of both the parents bill of rights and, with the Commissioner, model data security and privacy policies. Education Law § 2-d(3)(d), (5)(a).

As of June 11, 2014, the Commissioner had not announced the appointment of a Chief Privacy Officer.

Parents Bill of Rights

Section 2-d(3)(a) of the Education Law requires that each educational agency publish a "parents bill of rights for data privacy and security" on its website and include a copy of such document in every contract between the district and a third party contractor that receives student or educator data. The parents bill of rights will contain a series of protections and guarantees set forth in Section 2-d(3)(b), as well as "supplemental information for each contract an educational agency enters into with a third party contractor where the third party contractor receives student data or teacher or principal data." Education Law § 2-d(3)(c). This "supplemental information" is to be developed by the district, but must include the following:

- (1) The exclusive purposes for which the student data or teacher or principal data will be used;

- (2) How the third party contractor will ensure that the subcontractors, persons or entities that the third party contractor will share the student data or teacher or principal data with, if any, will abide by data protection and security requirements;
- (3) When the agreement expires and what happens to the student data or teacher or principal data upon expiration of the agreement;
- (4) If and how a parent, student, eligible student, teacher or principal may challenge the accuracy of the student data or teacher or principal data that is collected; and
- (5) Where the student data or teacher or principal data will be stored (described in such a manner as to protect data security), and the security protections taken to ensure such data will be protected, including whether such data will be encrypted.

While Education Law Section 2-d has been effective since March 31, 2014, the statute expressly states that the parents bill of rights for data privacy and security will be completed within 120 days after such date, or July 29, 2014. Education Law § 2-d(3)(d). This delay provides the Commissioner with time to solicit comments and promulgate regulations governing the parents bill of rights. In the interim, "The chief privacy officer, with input from parents and other education and expert stakeholders, shall develop additional elements of the parents bill of rights for data privacy and security." *Id.*

Given the timeline set forth in Section 2-d(3)(d) and the likelihood that the Commissioner's regulations will impose additional requirements, our office has not yet prepared a sample parents bill of rights. We will monitor the development of regulations and will provide additional information to subscribing districts as it becomes available.

Promoting the Least Intrusive Data Collection Policies Practicable

As part of the data privacy and security reforms imposed by the state legislature, SED is now required to promote responsible data collection policies, minimizing the collection and transmission of personally identifiable information and improving transparency in such practices. See Education Law § 2-d(4)(a). Specifically, the Chief Privacy Officer will be required to develop, regularly update, and make publicly available, "an inventory and understandable description of the student, teacher and principal data elements collected with an explanation and/or legal or regulatory authority outlining the reasons such data elements are collected and the intended uses and disclosures of the data." Education Law § 2-d(4)(b). The statute also furthers the aims of ensuring student, teacher, and principal privacy by prohibiting the sale or use of personally identifiable information maintained by educational agencies for marketing purposes, a point of concern for many opposed to recent actions taken or contemplated by SED. Education Law § 2-d(4)(f).

Data Security and Privacy Policies

In an effort to assist school districts in protecting sensitive information, the state legislature has required that SED develop data security and privacy policies that address parent access to student records. Education Law § 2-d(4)(g) expressly provides:

Parents shall have the right to inspect and review their child's educational record including any student data stored or maintained by an educational agency. *The department shall develop policies for school districts that:*

- (1) Provide for annual notification to parents of their right to request student data;
- (2) Ensure security when providing student data to parents, including that only authorized individuals receive such data; and

- (3) Specify a reasonable amount of time in which school districts should respond to such requests.

(Emphasis added).

In addition to developing the policies referenced above, the Commissioner will issue regulations establishing standards for educational agency data security and privacy policies, generally, and "develop one or more model policies for use by educational agencies." These standards and policies will be developed in consultation with the new Chief Privacy Officer, as well as experts from various fields, including security and cyber-security. Education Law § 2-d(5)(a). Once the Commissioner has developed and promulgated regulations, each school district must ensure it has a data security and privacy policy that complies with relevant state and federal laws and regulations. Pursuant to Section 2-d(5)(c), "Such policy shall be published on the educational agency's website, if it exists, and notice of such policy shall be provided to all officers and employees of the educational agency."

To date, our office has not prepared sample policies reflecting the provisions of either Section 2-d(4)(g) or Section 2-d(5)(a)-(c). As regards the former, the statute clearly places the obligation for developing such policies on SED, as opposed to school districts. Similarly, Section 2-d(5)(c) requires that school districts adopt new data security and privacy policies *after the promulgation of regulations*. As always, Erie 1 BOCES Policy Services will continue to monitor these issues and provide subscribers with additional information as it becomes available.

Disclosure of Personally Identifiable Information to Third Party Contractors

Section 2-d also imposes significant obligations with respect to school districts' disclosure of personally identifiable information to third party contractors. This is accomplished in three ways: (1) requiring that contracts between educational agencies and third party contractors contain provisions regarding confidentiality of student, teacher, and principal data, and incorporate a "data security and privacy plan" (including a signed copy of the parents bill of rights) ensuring such provisions are effectively implemented; (2) imposing a series of extra-contractual requirements on third party contractors (e.g., limiting internal access to education records, maintaining safeguards to protect the confidentiality of personally identifiable information, instituting mandatory reporting of security breaches, etc.); and (3) providing consequences for the failure to secure personally identifiable information. Education Law § 2-d(5)(d), *et seq.*

The above provisions are beyond the scope of policy insofar as they govern the terms of certain contracts and the consequences of breaching those agreements. Districts should consult their school attorneys as to the implementation of this law and how it might affect existing or prospective relationships with third party contractors.

Unauthorized Disclosure of Personally Identifiable Information

Finally, Section 2-d includes provisions aimed at addressing security breaches and other unauthorized disclosures of personally identifiable information. Specifically, the law requires that third party contractors notify a school district of any breach resulting in the unauthorized release of data "in the most expedient way possible and without unreasonable delay." Education Law § 2-d(6)(a). Upon receiving such notification, school districts are required to report the breach to the Chief Privacy Officer and the students, teachers, or principals whose personally identifiable information was improperly released. Education Law § 2-d(6)(a)-(b). The statute further provides that each breach and unauthorized release of student information is punishable by a civil penalty, and authorizes the Chief Privacy Officer to take action limiting an offending contractor's access to student, teacher, or principal data. Education Law § 2-d(6).

As discussed above, a number of provisions in Education Law § 2-d require that SED and the Commissioner of Education establish policies and promulgate regulations addressing data privacy and security. Meanwhile, other provisions specifically address issues that may be beyond the scope of policy, including relationships between third party contractors and educational agencies. In light of the legislature's decisions in drafting the law, our office is awaiting further guidance from SED before preparing sample policies or documents pertaining to the new law's provisions. We are, however, mindful that the parents bill of rights must be completed by July 29, 2014, and will provide updates prior to that time.

If you have any questions regarding the policy implications of Section 2-d, please do not hesitate to contact our office.

Policy Update Service

JoAnn Balazs, Director
Janell M. Hallgren, Manager
Carol M. Carlin
Karen A. DePalma
Patricia Ferrito
Jane Freer
Brian Hartmann, Esq.

Telephone: (716) 821-7072
Fax: (716) 821-7409

NOTE: This Alert is not to be interpreted as the rendering of legal advice. Questions regarding the application of law to specific situations should be directed to your school attorney.